REMARKS

Claims 1, 2, 4, 6, 8-10, 12, 13, 15, 17, 19-21, 34, and 47-49 are presented for examination, of which Claims 1, 9, 12, 20, 34, 47, and 49 are in independent form and have been amended to define still more clearly what Applicant regards as his invention. Claims 45 and 46 have been canceled, without prejudice or disclaimer of their subject matter, and will not be mentioned further. Favorable reconsideration is requested.

The most recent Office Action, dated May 24, 2004, among other things, rejected Claims 1, 2, 4, 5, 12, 13, 15, 34, and 47-49 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,189102 (*Beser*); and Claims 6, 8-10, 17, and 19-21 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Beser*, in view of U.S. Patent No. 5,850,388 (*Anderson et al.*).

As noted, Applicant has amended independent Claims 1, 9, 12, 20, 34, 47, and 49 in terms that more clearly define the present invention. Applicant submits that these amended independent claims, together with the remaining claims dependent thereon, are patentably distinct from the cited prior art for at least the following reasons..

The aspect of the present invention set forth in Claim 1 is a network apparatus that includes a receiving unit adapted to receive data from a network by using a predetermined protocol, and a detecting unit adapted to detect a predetermined value in a packet header of the data received by the receiving unit, the packet header being provided for the predetermined protocol. The apparatus also includes a setting unit adapted to set a destination logic address in a packet header of the received data as a logic address of the network apparatus in a case where (a) the predetermined value is detected by the detecting unit and (b) a destination

physical address of the received data and a physical address of the network apparatus are the same.

Among other notable features of Claim 1 is that when a predetermined value is detected in received data and when a destination physical address of the received data and a physical address of the network apparatus are the same, a destination logic address is set in a packet header of the received data as a logic address of the network apparatus. By virtue of this feature, the logic address can be set in the network apparatus using the destination logic address field in the packet header. Also, because the setting of the destination logic address as the logic address of the network apparatus is executed only when a predetermined value is detected in received data and when the destination physical address of the received data and the physical address of the network apparatus are the same, the setting of a logic address of unintended data in the network apparatus can be avoided.

As discussed previously, *Beser* relates to a method for authenticating network devices in a data-over-cable system. Figure 6 of *Beser* depicts a block diagram illustrating a Dynamic Host Configuration Protocol (DHCP) 66 message structure 108. The DHCP 66 message structure 108 includes, among other things, a client IP address field 124 (CIADDR), a your IP address field 126 (YIADDR), a server IP address field 128 (SIADDR), and a client hardware address field 132 (CHADDR). However, the DHCP 66 message structure does not indicate a destination address of the DHCP message. This is because the DHCP message is not transferred in accordance with the data in CIADDR, YIADDR, SIADDR, or CHADDR, and because the DHCP is located a layer higher than those of the Internet Control Message Protocol (ICMP) layer 56 and the Internet Protocol (IP) layer 54, as depicted in Figure 2.

Beser states, at Table 5 (column 15, lines 45-65), that when a network host client broadcasts a DHCPDISCOVER message on its local physical subnet, DHCP servers may respond with a DHCPOFFER message that includes an available network address in the YIADDR field, and that the DHCP servers unicast the DHCPOFFER message to the network host client, or may broadcast the message to a broadcast address on the client's subnet.

Beser, at column 18, lines 38-48, further states that in order to respond with the DHCPOFFER message to the network host client, the DHCP servers send the DHCPOFFER message to the address specified in the GIADDR field 130. Further, at column 19, lines 6-10, the cable modem CM 16 receives one or more DHCPOFFER messages from CMTS 12 on a downstream connection.

From the above cited passages, Applicant understands that the YIADDR of a DHCPOFFER message is an IP address that will be set in the CM, but is not an address that is set in a packet header as a destination address of the DHCPOFFER message. Applicant submits that *Beser* does not discuss setting the destination address in a packet header of received data as an address of the network apparatus itself. Accordingly, nothing has been found in *Beser* that would teach or suggest that when a predetermined value is detected in received data and when a destination physical address of the received data and a physical address of the network apparatus are the same, a destination logic address is set in a packet header of the received data as a logic address of the network apparatus, as recited in Claim 1.

Accordingly, Applicant submits that Claim 1 is not anticipated by *Beser*, and respectfully requests withdrawal of the rejection under 35 U.S.C. § 102(e).

Independent Claims 12 and 34 are method and network device control program claims, respectively, corresponding to apparatus Claim 1, and are believed to be patentable for at

least the same reasons as discussed above in connection with Claim 1. Additionally, independent Claims 47 and 49 include a feature substantially similar as that discussed above above in connection with Claim 1. Accordingly, Claims 47 and 49 are believed to be patentable for reasons substantially similar as those discussed above in connection with Claim 1.

The aspect of the present invention set forth in Claim 9 is a network apparatus. The apparatus includes a receiving unit adapted for receiving an ICMP echo message, a data length detecting unit adapted for detecting a data length in a packet header of the ICMP echo message received by the receiving unit, and a setting unit adapted for setting a destination IP address in an IP header of the received ICMP echo message as an IP address of the network apparatus if (a) the data length has a specific value and (b) a destination MAC address of the received ICMP echo message and a MAC address of the apparatus are the same.

Among other important features of Claim 9 is the network apparatus setting a destination IP address in an IP header of the received ICMP echo message as an IP address of the network apparatus if (a) the data length has a specific value and (b) a destination MAC address of the received ICMP echo message and a MAC address of the apparatus are the same.

As discussed above, in connection with Claim 1, the *Beser* method does not set the destination logic address of an IP header of the received data as the logic address of the network apparatus in a case where (a) the predetermined value is detected by the detecting unit and (b) a destination physical address of the received data and a physical address of the network apparatus are the same. For reasons substantially similar to those discussed above in connection with Claim 1, nothing has been found in *Beser* that would teach or suggest setting a destination IP address in an IP header of the received ICMP echo message as an IP address of the network apparatus if (a) the data length has a specific value and a destination MAC address of the

received ICMP echo message and (b) a MAC address of the apparatus are the same, as recited in Claim 9.

Accordingly, Applicant submits that Claim 9 is clearly allowable over *Beser*, taken alone.

Anderson et al. relates to protocol analyzers for monitoring and analyzing digital transmission networks. *Anderson et al.* is cited for allegedly teaching that the received data is an ICMP echo message by an ICMP protocol and that the special attribute is a data length of the ICMP echo message. However, nothing has been found in *Anderson et al.* that would teach or suggest setting a destination IP address in an IP header of the received ICMP echo message as an IP address of the network apparatus if (a) the data length has a specific value and (b) a destination MAC address of the received ICMP echo message and a MAC address of the apparatus are the same, as recited in Claim 9.

Therefore, even if *Beser* and *Anderson et al.* were to be combined in the manner proposed in the Office Action, assuming such combination would even be permissible or proper, the resulting combination also would fail to teach or suggest at least those features of Claim 9.

Accordingly, Applicant submits that Claim 9 is patentable over *Beser* and *Anderson et al.*, whether considered separately or in any proper combination.

Independent Claim 20 is a method claim corresponding to apparatus Claim 9, and is believed to be patentable for at least the same reasons as discussed above in connection with Claim 9.

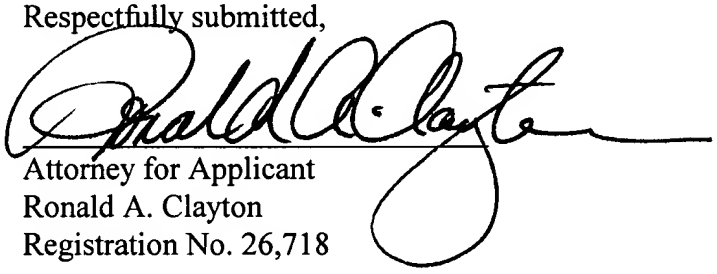
The other claims in this application are each dependent from one or another of the independent claims discussed above and are therefore believed patentable for the same

reasons. Since each dependent claim is also deemed to define an additional aspect of the invention, however, the individual reconsideration of the patentability of each on its own merits is respectfully requested.

In view of the foregoing amendments and remarks, Applicant respectfully requests favorable reconsideration and early passage to issue of the present application.

Applicant's undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our below listed address.

Respectfully submitted,



Attorney for Applicant
Ronald A. Clayton
Registration No. 26,718

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

NY_MAIN 484515v1